



## **User's Manual**

**Wireless LAN PCI Adapter**

**Model No.: SP906GK**

<http://www.micronet.info>

# CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Features.....	1
1.2	Specifications.....	1
1.3	Package Contents.....	2
<b>2</b>	<b>HARDWARE INSTALLATION .....</b>	<b>3</b>
<b>3</b>	<b>CONFIGURATION UTILITY .....</b>	<b>6</b>
3.1	Site Survey .....	9
3.2	Profile.....	9
3.2.1	Configure the Profile .....	11
3.2.1.1	Base Configuration.....	11
3.2.1.2	Wireless network security .....	12
3.2.1.3	802.1x Setting-Certification .....	16
3.2.1.4	802.1x Setting-CA Server .....	17
3.3	Advanced.....	19
3.4	Status.....	21
3.5	Statistics.....	22
3.6	Easy Config .....	22
3.7	Turbo Mode.....	22
<b>4</b>	<b>TROUBLESHOOTING.....</b>	<b>24</b>

# 1 Introduction

Thank you for purchasing the SP906GK. It complies with IEEE 802.11g standard and supports up to 54Mbps high-speed wireless network connections. It can also work with IEEE 802.11b devices. When SP906GK is connected to 11b devices, the link speed will be up to 11Mbps.

It enables higher data throughput than the IEEE 802.11g standard (up to 54Mbps) and supports specific ways to increase the data transfer rate for a time by compressing the data and decreasing the waiting time to send the next data to the Routers or APs in Turbo Mode. When SP906GK is connected to the Routers or APs with the proprietary Turbo Mode feature, the wireless network will be even more efficient.

For WLAN security issues, SP906GK supports 64/128-bit WEP data encryption that protects your wireless network from eavesdropping. It also supports WPA (Wi-Fi Protected Access) feature that combines IEEE 802.1x and TKIP (Temporal Key Integrity Protocol) technologies. Client user authorization is required before accessing to APs or AP Routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key. Furthermore, SP906GK supports AES function, offering a stronger encryption mechanism, which is often required by corporate and government users.

SP906GK power consumption is also very low. SP906GK has several levels of power saving modes, allowing user to customize from portable or handheld devices the way he/she wishes to save power.

With its various features and ability to support advanced technology, SP906GK is the most cost-effective solution to build your wireless network.

## 1.1 Features

- Comply with the IEEE 802.11b and IEEE 802.11g standards.
- High-speed wireless transfer data rate - up to 54Mbps.
- Provide high level of security with 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 (AES with IEEE 802.1x) functions
- Provide automatic fallback for greater data security and reliability.
- Supports Windows 98SE/Me/2000/XP operating systems
- Supports 32-bit PCI interface.

## 1.2 Specifications

- Standard: IEEE 802.11b/g
- Interface: 32-bit PCI
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)
- BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP Data Encryption, WPA (TKIP with IEEE 802.1x), WPA2 (AES with IEEE 802.1x) Note: WPA2 is only enabled in Windows 2000/XP.
- Antenna: Printed Antenna with Diversity System
- Drivers: Windows 98SE/Me/2000/XP
- LEDs: Link, Activity
- Transmit Power: 16dBm~18dBm
- Dimension: 8(H) x 118(W) x 54(D) mm
- Temperature: 32~131°F (0 ~ 55°C)
- Humidity: Max. 95% (NonCondensing)
- Certification: FCC, CE

### **1.3 Package Contents**

Before you begin the installation, please check the items in your package. The package should include the following items:

- Micronet SP906GK Wireless LAN PCI Adapter
- Driver and Manual CD
- Quick Installation Guide
- Detachable Antenna

***If any of the above items is missing, contact your supplier as soon as possible.***

## 2 Hardware Installation

Before you proceed with the installation, please read the following notes carefully:

**Note1:** Please do not install SP906GK into your laptop computer before installing the software program from the CD.

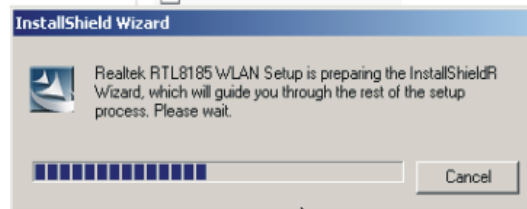
**Note2:** The following installation was performed under Windows XP. (Procedures are similar for Windows 98SE/Me/2000.)

**Note3:** If you have installed the SP906GK Wireless PCI Adapter driver & utility before, please uninstall the old version first.

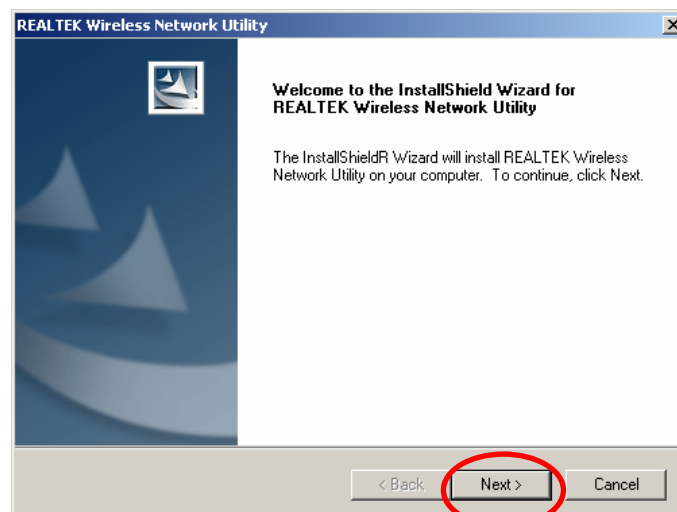
- A. Insert the Installation CD to your CD-ROM Drive. Execute the “setup” program. (/Utility and Driver/setup.exe)



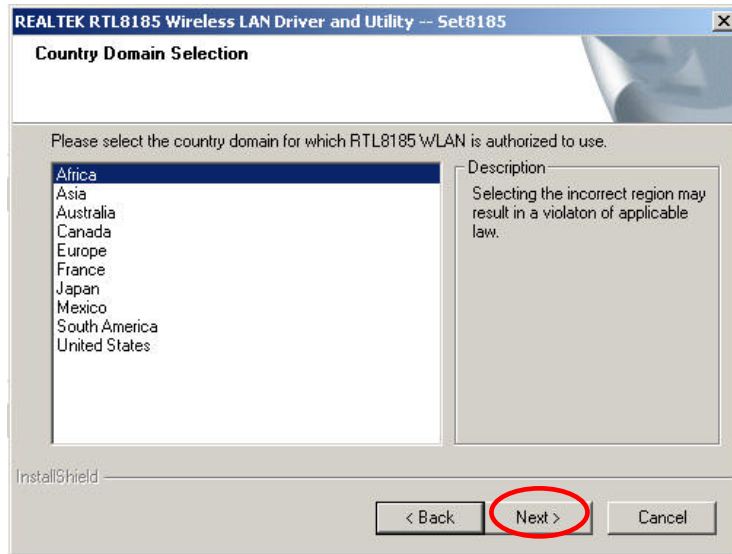
- B. The “InstallShield Wizard” will start automatically.



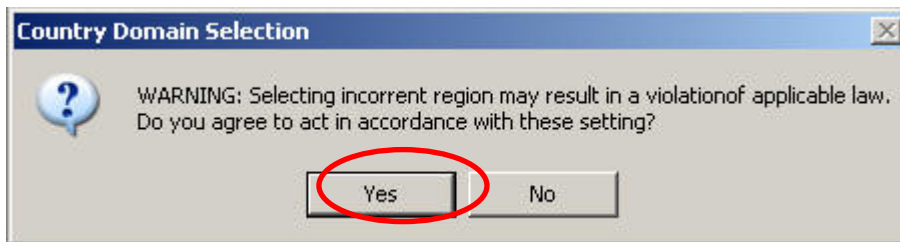
- C. Click “Next” to install utility.



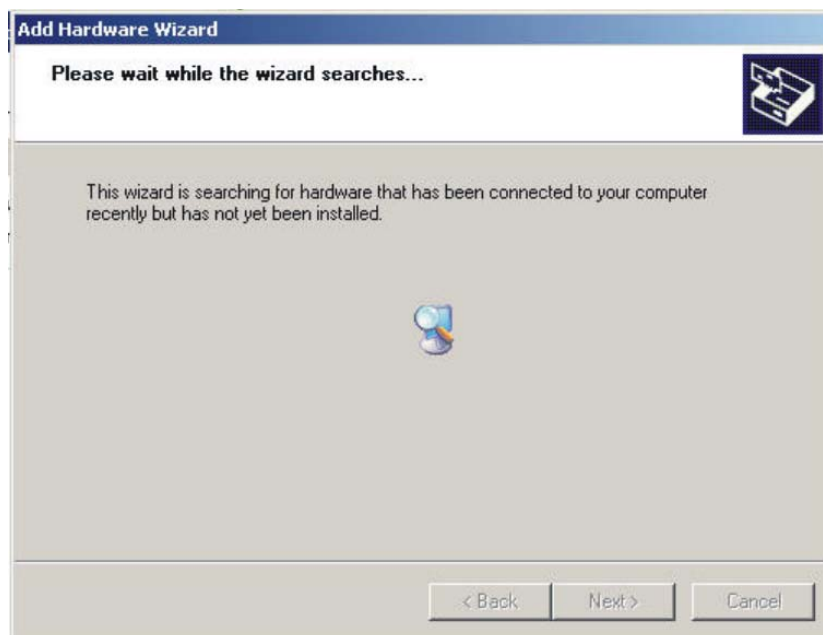
D. After selecting the country domain, click “Next” to process the installation..



E. **Warning: Selecting incorrect region may result in a violation of applicable law** dialog window will pop-up. If you have selected the correct region, click “Yes” continue the process.

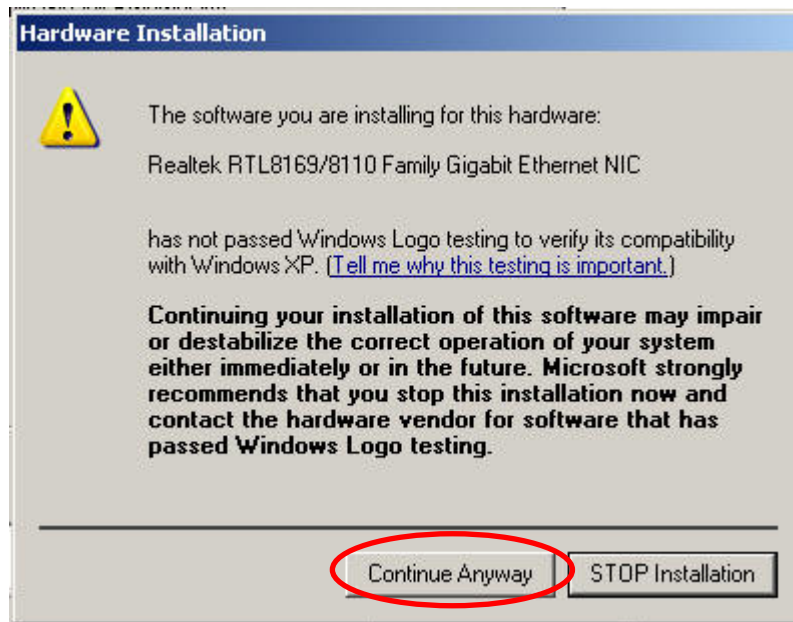


F. The system will start to install the software of SP906GK . Follow the instruction of the program and plug in SP906GK into the PCI slot of your desktop computer.

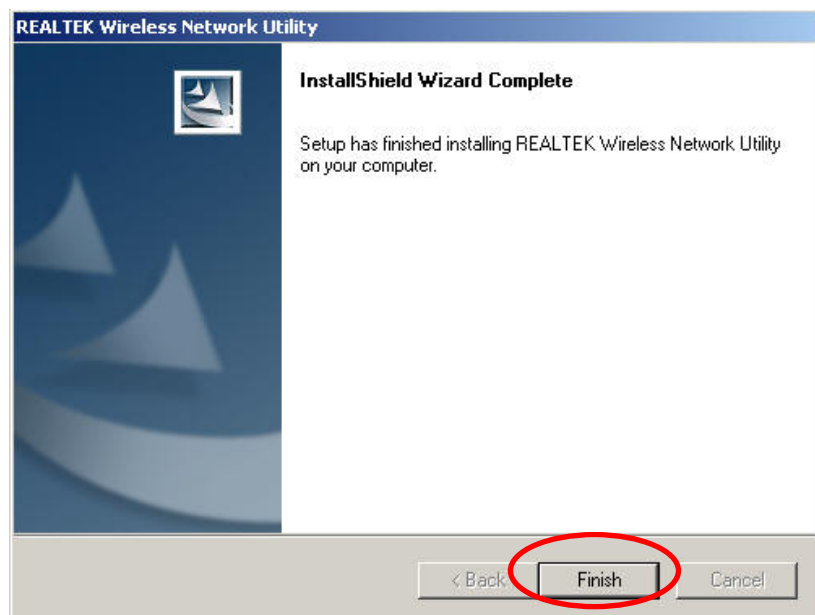




G. The system will automatically detect SP906GK and display the “**Hardware Installation**” screen. Click “**Continue Anyway**” to continue.



H. Click “**Finish**” to complete the installation.

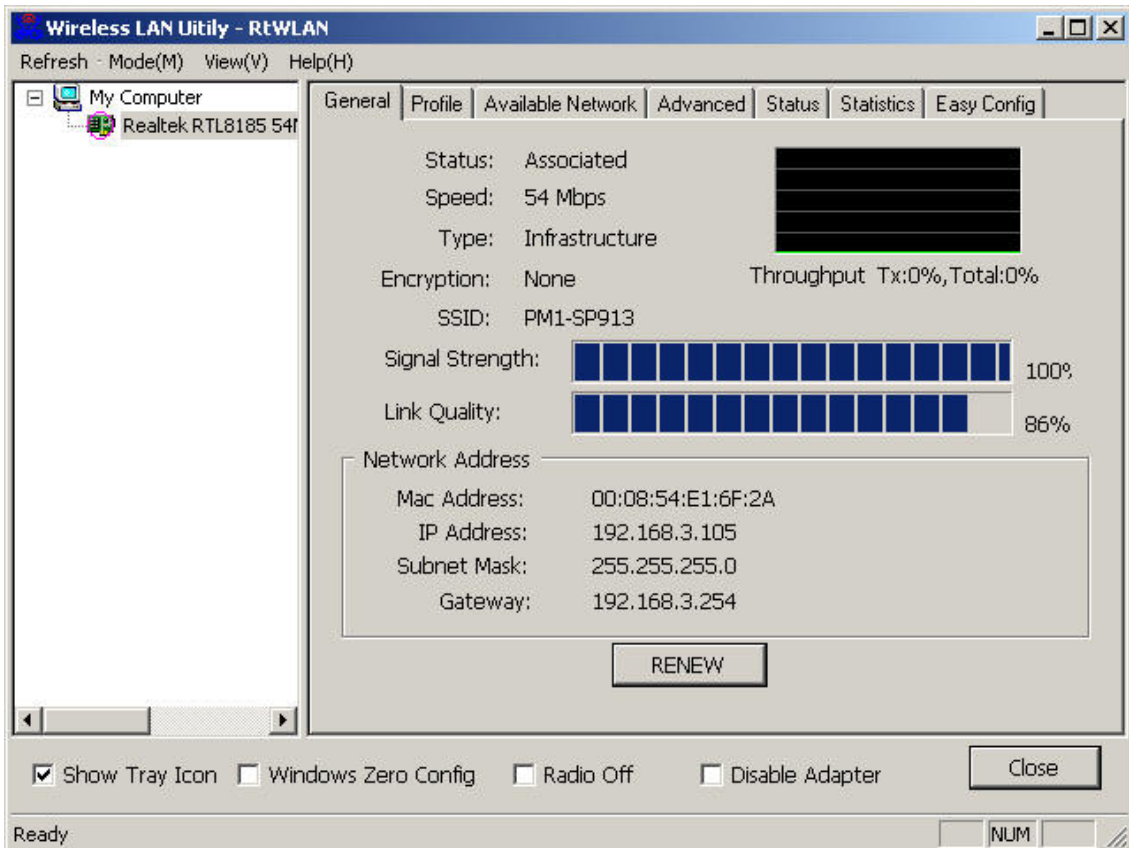




### 3 Configuration Utility

The Configuration Utility is a powerful application that helps you configure SP906GK and monitor the link status and the statistics during the communication process.

If SP906GK is installed successfully, the configuration utility will automatically pop up. It will automatically connect to the wireless device, which has better signal strength and no wireless security setting.

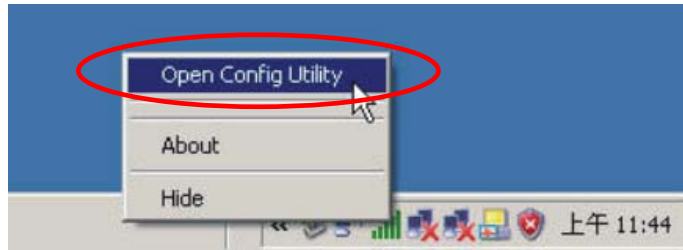


The Configuration Utility appears as an icon on the system tray of Windows while SP906GK is running. You can double-click on the icon to open the utility.



Right click the icon to find the items in configuration utility for you to perform.

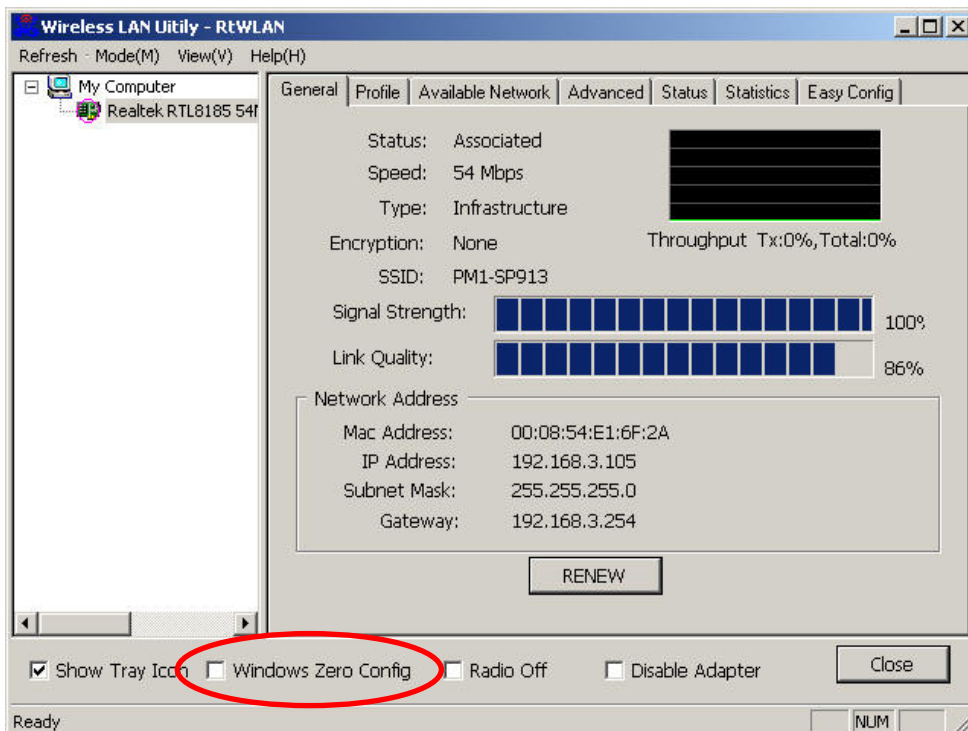
- Launch Config Utilities  
Select “**Open Config Utility**” to open the Configuration Utility tool.
- Use Zero Configuration as Configuration Utility
- Select “**About**” to describe the Wireless Card information.
- Hide  
Select “**Hide**” to hide the Configuration Utility tool.



In Windows XP, there is a “**Windows Zero Configuration Tool**” for you to set up wireless clients. By default, this “**Windows Zero Configuration Tool**” is enabled. You can use the Utility for the card by one of the following methods:

### Method 1

Double click the icon in the system tray and disable “**Window Zero Config**”.

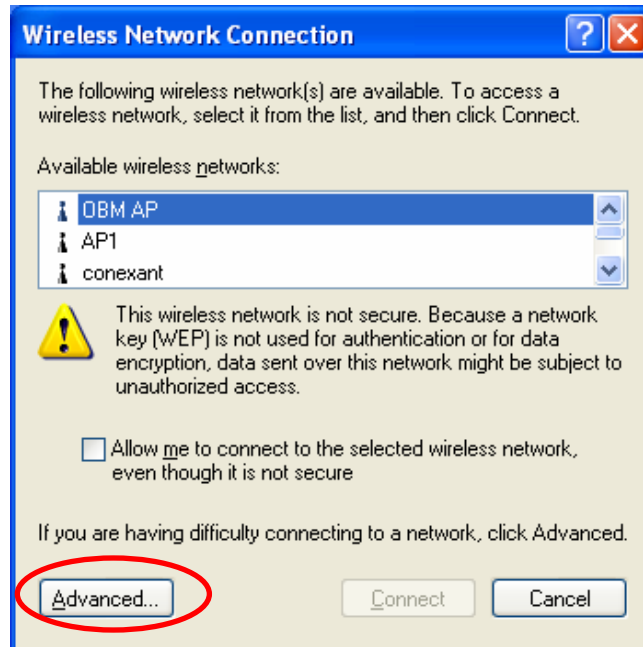


### Method 2

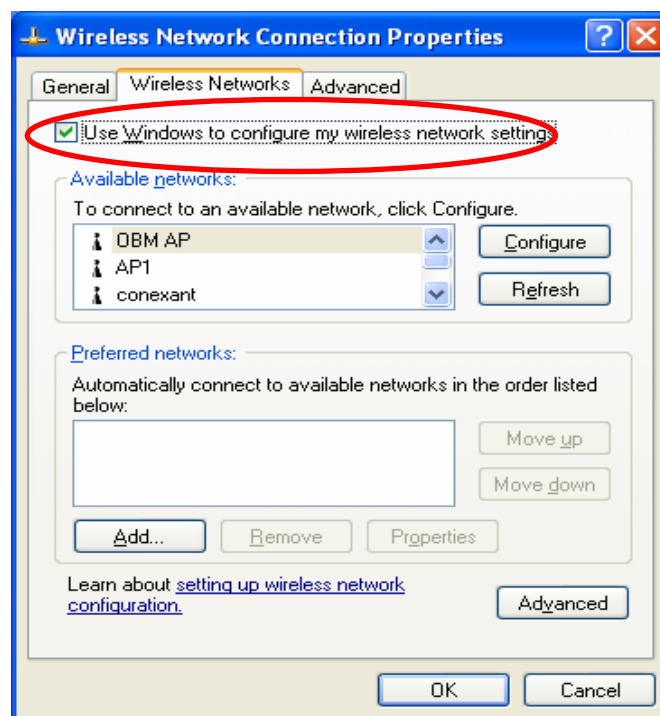
A. Right-click the icon and select “**View Available Wireless Networks**”.



B. Click “Advanced”.



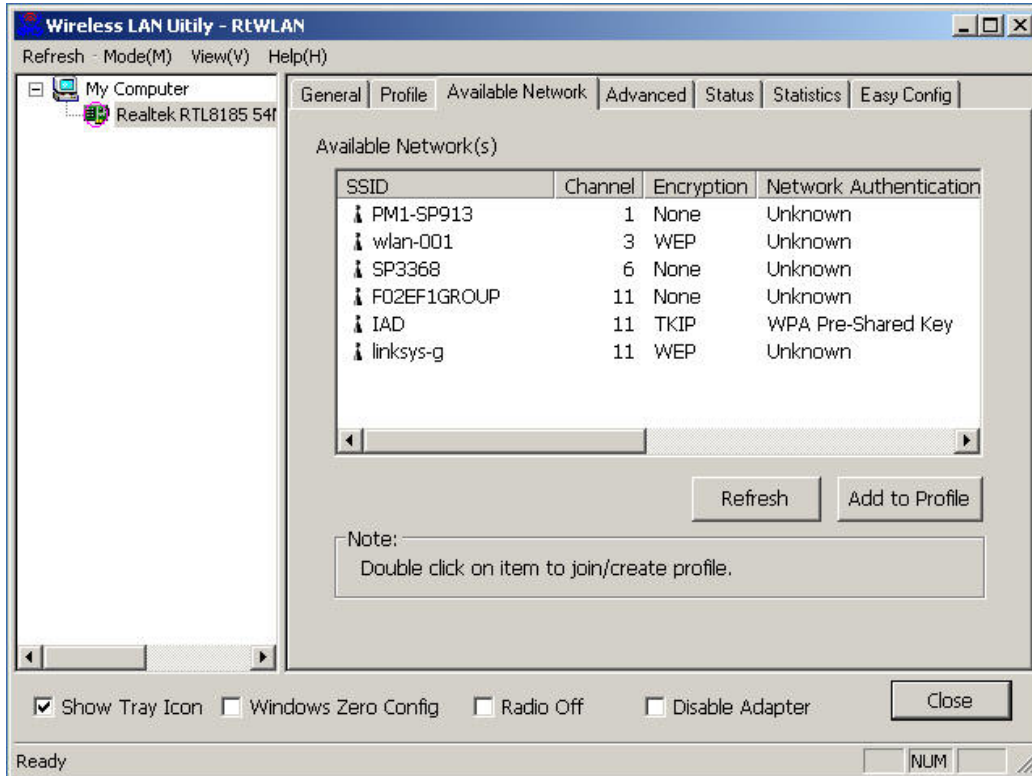
C. Uncheck “Use Windows to configure my wireless network settings” to enable the utility for the card.



**Note:** If “Wireless Zero Configuration” is enabled, you can only configure the advance setting or check the link status and statistics from the configuration utility of the card.

### 3.1 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of SP906GK and automatically connect you to the wireless device with the greatest signal strength. The “**Available Network**” will list all the networks nearby. You can change the connection to another AP or add one of the APs to your own profile list.

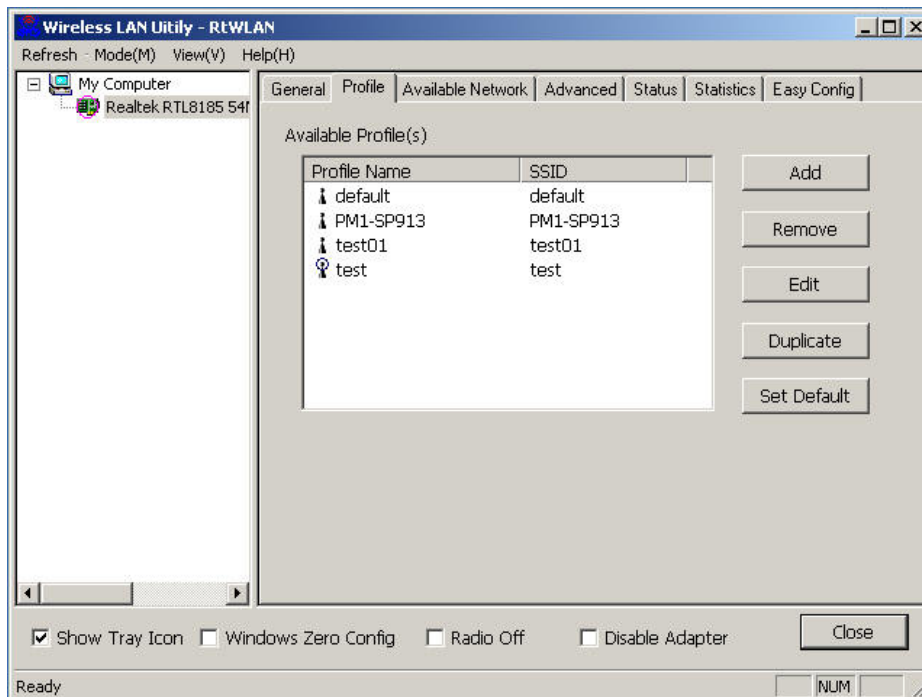




Parameter	Description
Available Networks	This list shows all available wireless networks within range of your card. It also displays the information of the networks including the SSID, BSSID, Signal Strength, Channel, Encryption, Authentication and Network Type. If you want to connect to any networks on the list, double-click the item on the list, and SP906GK will automatically connect to the selected network.
Refresh Button	Click “ <b>Refresh</b> ” button to collect the new information of all the wireless networks nearby.
Add to Profile Button	Add the selected network to Profiles list.

### 3.2 Profile

The “**Profile List**” allows you to manage the networks you connect to frequently by

## Add/Delete/Edit/Activate a profile.



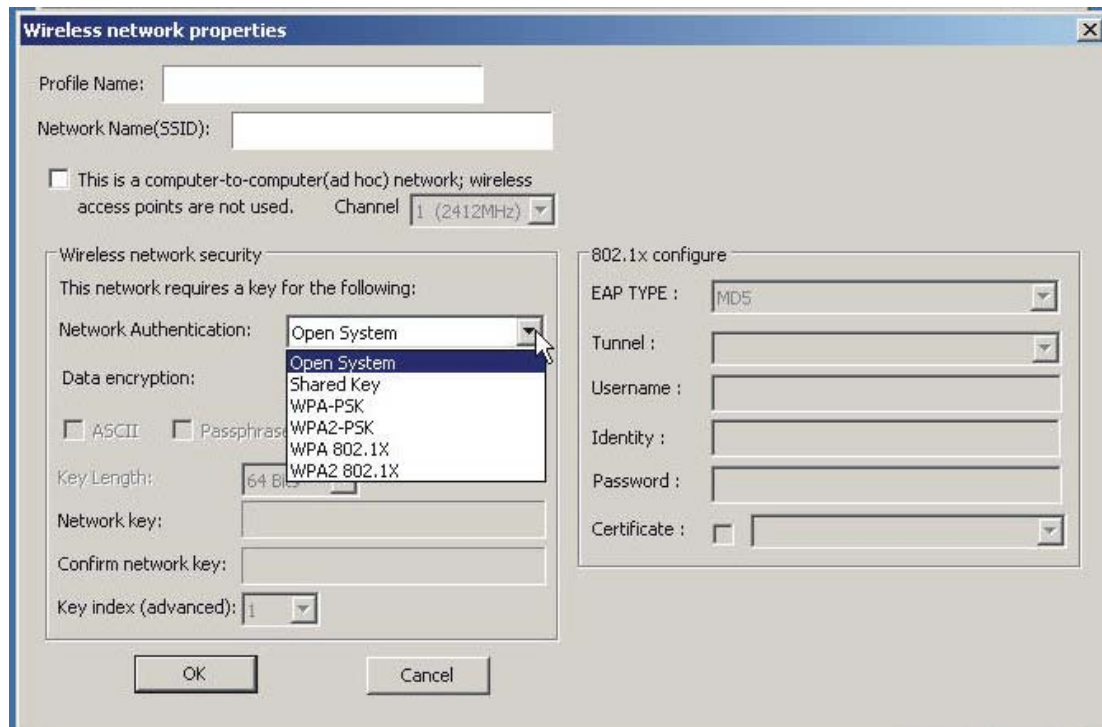
Parameter	Description
Profile List	<p>The profile list displays all the profiles and their relative settings including <b>Profile Name</b>, <b>SSID</b>.</p> <p> This sign indicates the activated profile is <b>connecting</b>.</p> <p> This sign indicates the activated profile is <b>disconnected</b>.</p>
Add/Remove/Edit/Duplicate/Set Default Button	Click these buttons to <b>Add / Remove / Edit / Duplicate / Set Default</b> the selected profiles.

## 3.2.1 Configure the Profile

### 3.2.1.1 Base Configuration

Parameter	Description
Profile Name	Define a recognizable profile name for you to identify the different networks.
SSID	<p>The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.</p> <p>You may specify a SSID for SP906GK and then only the device with the same SSID can interconnect to the card. If you want to add the network nearby to the profile list, pull down the menu, and all the networks will be listed for you to select from to add to the profile list.</p>
Channel	<b>This is a computer to computer (Ad Hoc) network; wireless access points are not used.</b> You could configure the channel range from <b>1</b> to <b>11</b> .

### 3.2.1.2 Wireless network security



Parameter	Description
Network Authentication Type	<p>This setting has to be consistent with the wireless networks that SP906GK intends to connect.</p> <p><b>Open System</b> – No authentication is needed in the wireless network.</p> <p><b>Shared Key</b> – Only wireless devices using a shared key (WEP Key identified) are allowed to connect to each other.</p> <p><b>WPA</b> – WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging the existing authentication databases and infrastructure.</p> <p><b>WPA-PSK</b> – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting</p>

---

password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

**WPA2** – Like WPA, WPA2 supports IEEE 802.1 x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required by the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

**WPA2-PSK** – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).

**WPA 802.1X** – Set the wireless devices using a WPA 802.1X mode

**WPA2 802.1X** – Set the wireless devices using a WPA2 802.1X mode

---

Data encryption

**None** – Disable the encryption mode.

**WEP** – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys.

**TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This ensures much greater security than the standard WEP security.

**AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and is the most advanced solution defined by IEEE 802.11i for security in the wireless network.

Note: All devices in the network should use the same encryption method to ensure the communication.

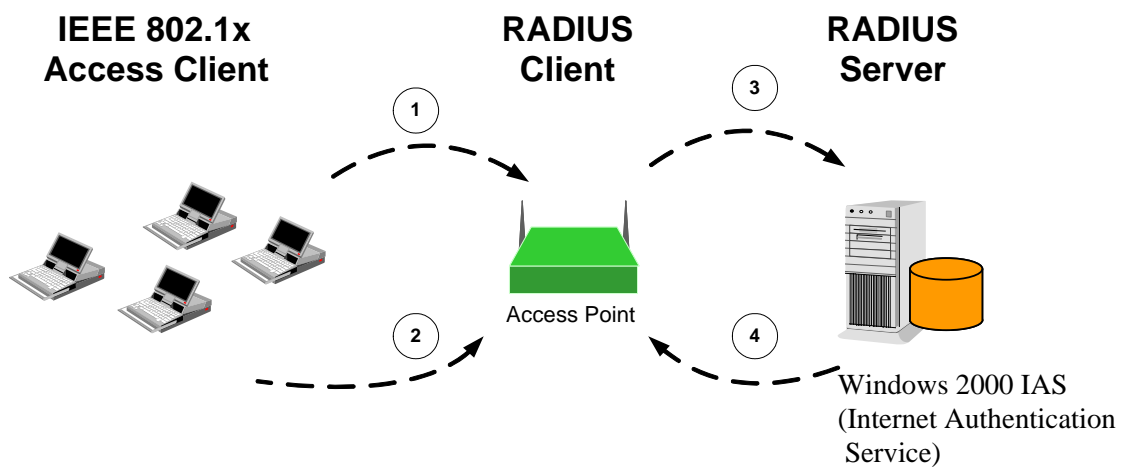


802.1x Setting	When you set the Authentication Type to Open, Shared, WPA or WPA2, you can also enable IEEE 802.1x setting to use the authentication server or certification server to authenticate client users.
WPA Pre-Shared Key	The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
WEP Key (Key1 ~ Key4)	<p>The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Select the default encryption key from Key 1 to Key 4 by selected the radio button.</p> <p>Fill the text box by as instructed below:</p> <p><b>64-bit</b> – Input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII characters (including “a-z” and “0-9”) as the encryption keys. For example: “0123456aef” or “test1”.</p> <p><b>128-bit</b> – Input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 13-digit ASCII characters (including “a-z” and “0-9”) as the encryption keys. For example: “01234567890123456789abcdef” or “administrator”.</p>

The **IEEE 802.1X** specification describes a protocol used for authenticating both clients and servers on a network. The authentication algorithms and methods are those provided by the **Extensible Authentication Protocol (EAP)**, a method of authentication that has been in use for a number of years on networks that provide **Point-to-Point Protocol (PPP)** support as many internet service providers and enterprises do.

When an AP acting as an authenticator detects a wireless station on the LAN, it sends an EAP-Request for the user's identity to the device. (**EAP**, the Extensible Authentication Protocol, is an authentication protocol that runs before network layer protocols transmit data over the link.) In turn, the device responds with its identity, and the AP relays this identity to an authentication server, which is typically an external **RADIUS** server.

### An example for MD5 Authentication



**(1) Client requests to login the network.**

**(2) Login with username, password.**

**(3) Send username, password to RADIUS server.**

**(4) Approve or deny user login to the LAN.**

### 3.2.1.3 802.1x Setting-Certification

802.1x configure

EAP TYPE : MD5

Tunnel :

Username :

Identity :

Password :

Certificate :

Parameter	Description
Authentication Type	<p>The EAP authentication protocols this card supports are listed below. This setting has to be consistent with the wireless APs or Routers that SP906GK intends to connect.</p> <p><b>PEAP &amp; TTLS</b> – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol to be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MS-CHAP, MS-CHAPv2, PAP and EAP-MD5. PEAP specifies that an EAP-compliant authentication protocol must be used; this card supports EAP-MSCHAP v2, EAP-TLS/Smart card and Generic Token Card. The client certificate is optional for authentication needs.</p> <p><b>TLS/Smart Card</b> – TLS is the most secure of the EAP protocols but is not easy to use. It requires exchanging digital certificates in the authentication phase. The server presents a certificate to the client. After validating the server's certificate, the client will then present a client certificate to the server for validation.</p> <p><b>MD5-Challenge</b> – MD5-Challenge is the easiest EAP Type. It requires the wireless station to enter a set of user name and password as the identity to RADIUS Server.</p>

Session Resumption	Select from “Disabled”, “Reauthentication”, “Roaming”, “SameSSID” and “Always” options when you want to recover the session in different status.
Identity	Name the server for server identification.
Password	Enter the password for server identification.
Use Client Certificate	A client certificate is required for TLS, and is optional for TTLS and PEAP. This item forces a client certificate to be selected from the appropriate Windows Certificate Store and made available to the RADIUS server for certification.

---

### **Tunneled Authentication**

Protocol	When the authentication type is PEAP or TTLS, select a protocol for building the encrypted tunnel.
Identity	This is the protected user EAP Identity used for authentication. The identity specified may contain up to 63 ASCII characters, is case sensitive and takes the form of a Network Access Identifier, consisting of <name of the user>@<user’s home realm>. The user’s home realm is optional and indicates the routing domain.
Password	The password used for authentication. It may contain up to 63 ASCII characters and is case sensitive.

---

#### **3.2.1.4 802.1x Setting-CA Server**

<b>Parameter</b>	<b>Description</b>
Use Certificate Chain	When the EAP authentication type such as TLS, TTLS or PEAP is selected and requires a certification to tell the client what server credentials to accept from the authentication server in order to verify the server, you have to enable this function.
Certificate Issuer	Choose the server from the list to issue the certificate. If “ <b>Any Trusted CA</b> ” is selected, any CA included on the list (provided by the Microsoft Certificate Store) will be permitted.

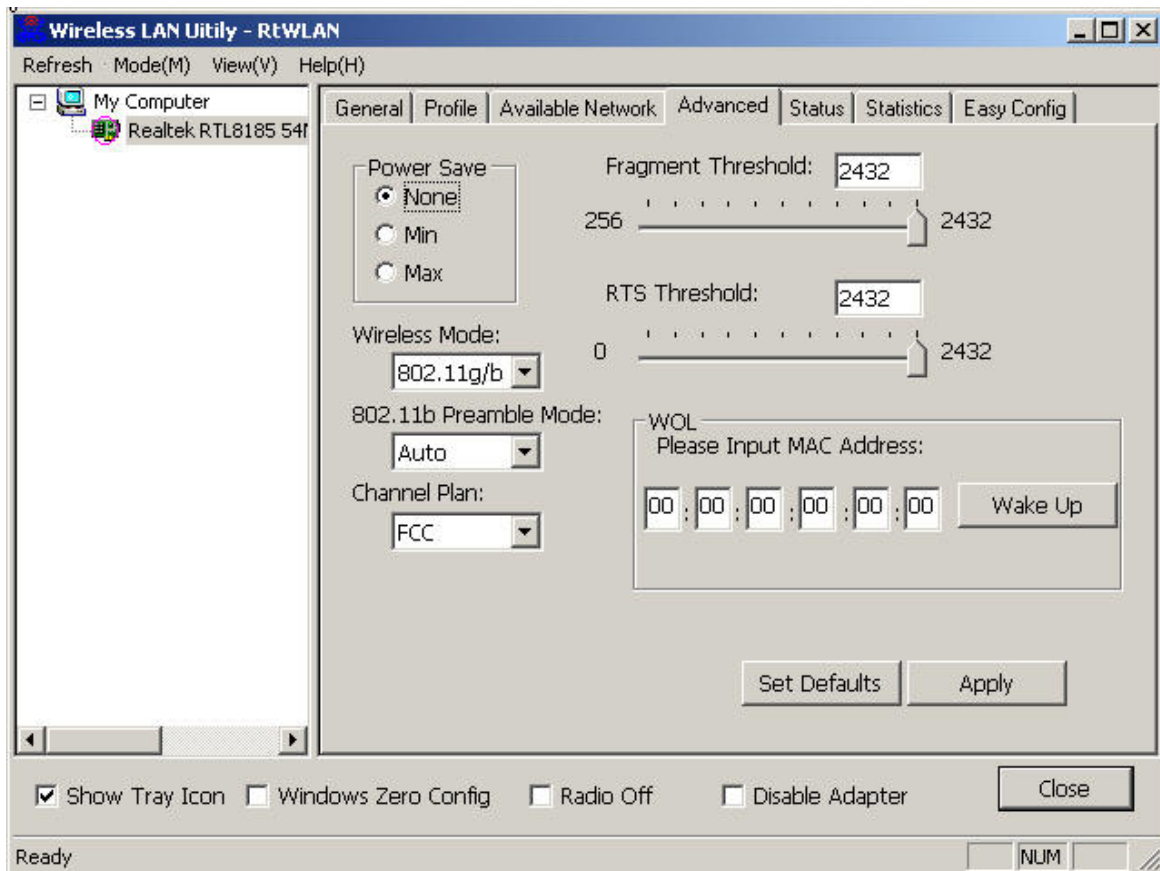
---

---

Allow Intermediate Certificates	When the server designates an issuer as a trusted root authority, it places the issuer's self-signed certificate, which contains the issuer's public key, into the trusted root certification authority certificate store of the host computer. Intermediate or subordinate certification authorities are trusted only if they have a valid certification path from a trusted root certification authority.
Server Name	Enter the authentication server name.
Server name must match exactly	When selected, the server name must match exactly with the server name found on the certificate.
Domain name must end in specified name	When selected, the server name field will identify a domain. The certificate must use a server name belonging to this domain or to one of its sub-domains (e.g. zeelans.com, where the server is blueberry.zeelans.com) but it may be any name used in the certificate name field.

---

### 3.3 Advanced

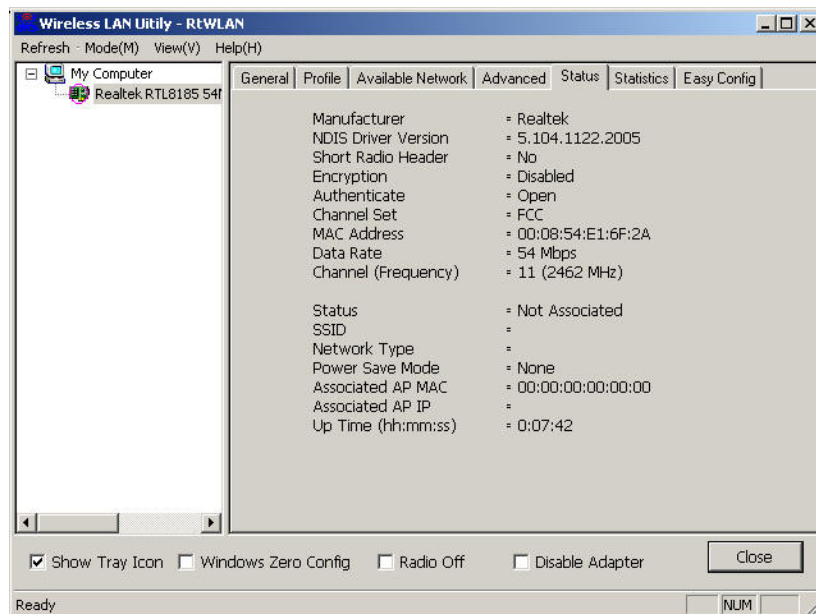


Parameter	Description
PSM (Power Save Mode)	<p>The power saving function is only available when the network type is in Infrastructure.</p> <p><b>None</b> – Disable the Power Save mode.</p> <p><b>Min</b> – SP906GK will always set in Minimum mode.</p> <p><b>Max</b> – SP906GK will always set in Maximum mode</p>
Wireless Mode	<p>SP906GK can be compatible with both 802.11g and 802.11b wireless stations</p> <p><b>802.11 B only</b> – If there are only 802.11b wireless stations in the network, you can set SP906GK to this mode.</p> <p><b>802.11 B/G mix</b> – If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended that SP906GK is set to this mode. This mode is also the default setting.</p>

Preamble	<p>The preamble defines the length of the CRC block for communication among wireless devices. This option is only active in the Ad Hoc network.</p> <p>There are three modes including Auto, Short and Long Preamble. If “<b>Auto</b>“mode is selected, SP906GK will automatically switch the preamble mode depending on the wireless devices SP906GK is connected to.</p> <hr/>
RTS Threshold	<p>Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent, and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2347 bytes. Minor change is recommended.</p>
Fragment Threshold	<p>The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you decreased this value and experienced high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2346 bytes. Minor change is recommended.</p>
Channel Plan	<p>This setting allows you to choose the certificate of country or organization.</p>

### 3.4 Status

From the “**Status**” option, you can view all the information of the network you are connected to.

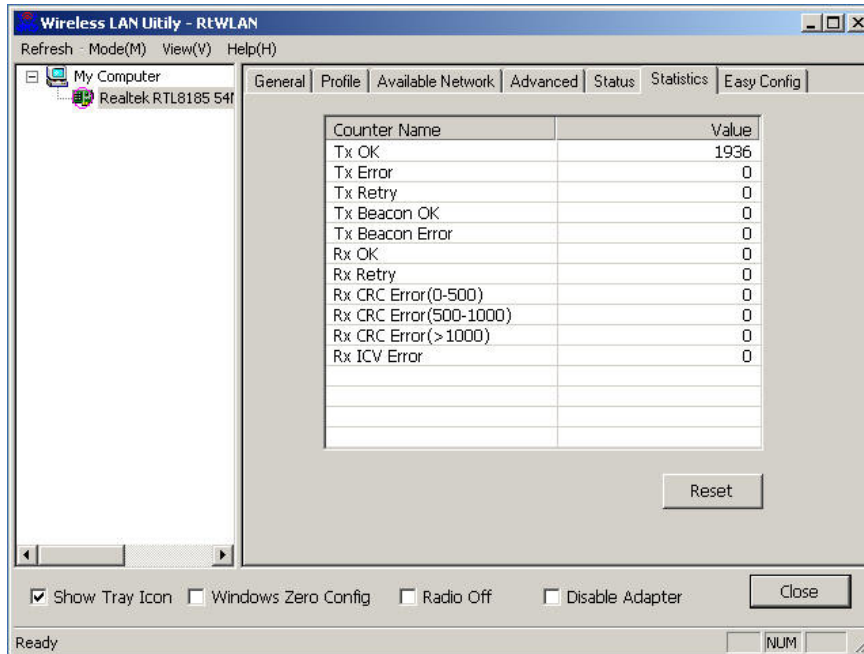


Parameter	Description
Manufacturer	Display the Chip-set manufacturer.
NDIS Driver Version	Display Current Driver version.
Short Radio Header	Display the Short Radio Header.
Encryption	Display the encryption method used on SP906GK
Authenticate	Display the Authentication method configured on SP906GK
Channel Set	Display the Certification of channel plan.
MAC Address	Display the MAC address of SP906GK.
Data Rate (Mbps)	Display the transmission and reception rate of the network. The maximum transmission rate is 54Mbps.
Channel	Display the number of the radio channels and the frequency used for the networking.



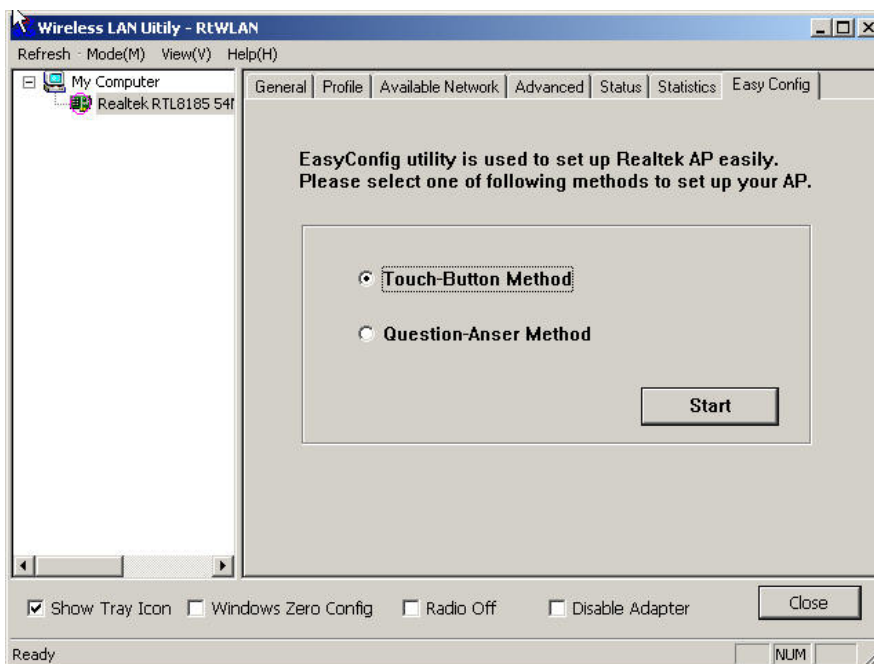
### 3.5 Statistics

This option enables you to view the statistic information of the connection, including transmit statistics and receive statistics. You may click the “**Reset**” to reset the SP906GK counters.



### 3.6 Easy Config

This option offers you two methods to configure SP906GK easily; select **Touch-Button Method** or **Question-Answer Method**. Then click “**Start**”.



### 3.7 Turbo Mode

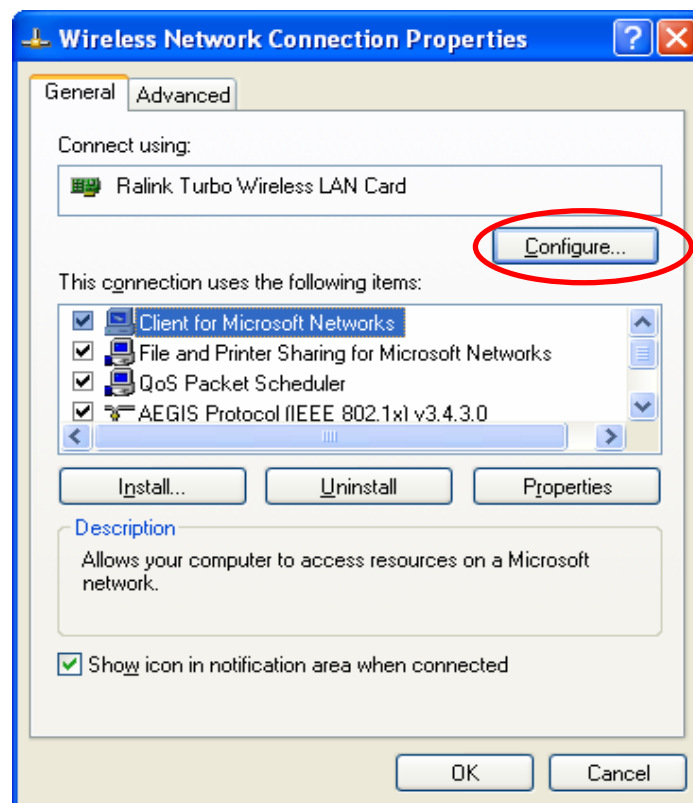
SP906GK supports specific ways to increase the data transfer rate at a time by

compressing the data and decreasing the waiting time for sending the next data to the Routers or APs. This feature (known as Turbo Mode) enables higher throughput than IEEE 802.11g standard (Up to 54Mbps).

When SP906GK is connecting to the Routers or APs with the proprietary Turbo Mode feature, the Turbo Mode will be enabled automatically without any configuration.

A. Right Click the “**Wireless Network Connection**” and select “**Properties**”.

B. Click “**Configure...**”.



C. Select “**Advanced**” page, enable the “**Turbo mode**”.

## 4 Troubleshooting

This chapter provides solutions to problems commonly encountered during the installation and operation of the adapter.

### 1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications which provides up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream in wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

- A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.
- B. A protection mechanism called RTS/CTS governs how 802.11g devices and 802.11b devices interoperate.

### 2. What is the IEEE 802.11b standard ?

The IEEE 802.11b Wireless LAN standard subcommittee formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

### 3. What does IEEE 802.11 feature support ?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

### 4. What is Ad-hoc ?

An Ad-hoc integrated wireless LAN is a group of computers, each having a Wireless LAN adapter, connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

### 5. What is Infrastructure ?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central

database, or wireless application for mobile workers.

**6. What is BSS ID ?**

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

**7. What is WEP ?**

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

**8. What is TKIP?**

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP involves IEEE 802.11i WLAN security standard.

**9. What is AES?**

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

**10. Can Wireless products support printer sharing ?**

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

**11. Would the information be intercepted while transmitting on air ?**

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up based on their needs.

**12. What is DSSS ? What is FHSS ? And what are their differences ?**

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

### **13. What is Spread Spectrum ?**

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secured, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal would look like background noise. There are two main types: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Copyright 2006 Micronet Communications, Inc. All rights reserved. No Part of the contents of this guide maybe transmitted or reproduced in any form or by any means without the written permission of manufacturer. Printed in Taiwan.

### **FCC Statement**

This product has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used according to the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her owns expense will be required to take whatever measures may be required to correct the interference.

### **FCC Caution**

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

### **Federal Communications Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

### **Federal Communications Commission (FCC) RF Exposure Requirements**

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for Certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such a PDAs or lappads is not authorized. This transmitter is restricted for use with the specific antenna(s) tested in the application for Certification. The antenna(s) used for this

transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

### **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

### **CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.